PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-153015
(43)Date of publication of application : 10.06.1997

(51)Int.Cl. G06F 15/00
H04L 9/32
H04N 7/167

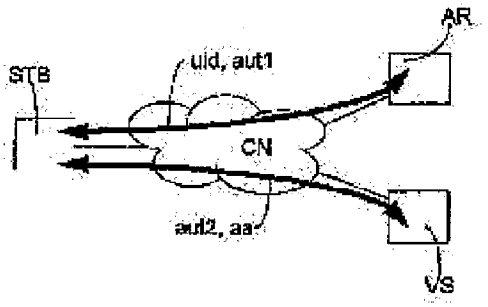
(21)Application number : 08-253148
(22)Date of filing : 25.09.1996

(71)Applicant : SIEMENS AG
(72)Inventor : HUSSMANN HEINRICH DR

(30)Priority
Priority number : 95 19535635 Priority date : 26.09.1995 Priority country : DE

(54) ELECTRONIC INFORMATION SERVICE UNDER GUARANTEE OF USER SECRECY FOR ELECTRONIC INFORMATION SERVICE OPERATOR

(57)Abstract:
PROBLEM TO BE SOLVED: To enable the use of electronic information service under the guarantee of secrecy of a user for an operator by transmitting use qualification information which does not include user identification information data to the user by an authentication server.
SOLUTION: Between the communication terminal equipment (STB) of a user, an information sever (VS) and an authentication server (AR), a connection path is formed via a communication network (CN) and identification information is transmitted from the STB to the AR. From the AR, use qualification (fair use power) information is transmitted to the ST. This use qualification information does not include the information on the identification of a user. This use qualification information is transmitted from the STB to the VS. Then, the VS checks the use qualification information and permits the use of information service when the positive result (correct) of a correct/error decision check is performed. Thus, the secrecy of the identification of the user for a video service operator becomes possible and the charge settlement of accounts or the charging of the cost according to a use status is possible.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－153015

(43)公開日　平成9年(1997)6月10日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　15/00	３３０		Ｇ０６Ｆ　15/00	３３０Ｂ	
Ｈ０４Ｌ　9/32			Ｈ０４Ｌ　9/00	６７３Ａ	
Ｈ０４Ｎ　7/167			Ｈ０４Ｎ　7/167	Ｚ	

審査請求　未請求　請求項の数9　ＯＬ　（全 6 頁）

(21)出願番号　特願平8－253148

(22)出願日　平成8年(1996)9月25日

(31)優先権主張番号　１９５３５６３５．７

(32)優先日　1995年9月26日

(33)優先権主張国　ドイツ（ＤＥ）

(71)出願人　390039413
シーメンス　アクチエンゲゼルシヤフト
ＳＩＥＭＥＮＳ　ＡＫＴＩＥＮＧＥＳＥＬＬＳＣＨＡＦＴ
ドイツ連邦共和国　ベルリン　及び　ミュンヘン　（番地なし）

(72)発明者　ハインリッヒ　フスマン
ドイツ連邦共和国　トゥッツィング　ハインリッヒ－フォークルーシュトラーセ　10

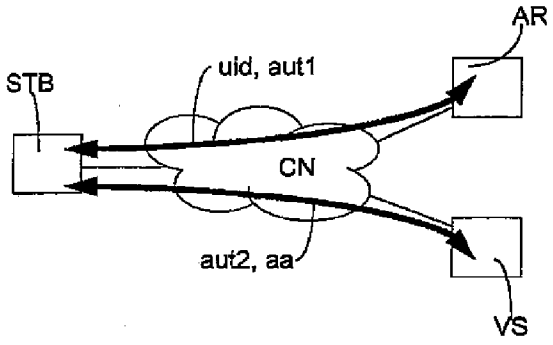
(74)代理人　弁理士　矢野　敏雄　（外２名）

(54)【発明の名称】　電子的情報サービス運用者に対するユーザの秘匿性の確保下で電子的情報サービスを利用する方法

(57)【要約】

【目的】　電子的情報サービス運用者に対するユーザの秘匿性の確保下で電子的情報サービスを利用する有効な方法を提供すること。

【構成】　相互通信型（対話型）ビデオサービスの利用中心の料金決済（清算）のもとで、電子的情報サービス運用者に対して、ユーザの識別性を秘密にすること（秘匿性）を確保することを可能にするため、顧客の識別性に関して知識を取得（知得）するがビデオサービスにおける利用関係（関連）事項特性についての情報を含まない認証（許可）サーバを使用すること。



1

【特許請求の範囲】

【請求項1】　電子的情報サービス運用者に対するユーザの秘匿性の確保下で電子的情報サービスを利用する方法において、

a）ユーザの通信端末装置（ＳＴＢ）と情報サーバ（ＶＳ）との間に接続（路）を、通信ネットワーク（ＣＮ）を介して形成し、

b）　ユーザの通信端末装置（ＳＴＢ）と認証サーバ（ＡＲ）との間に接続（路）を、通信ネットワーク（ＣＮ）を介して形成し、

c）ユーザの通信端末装置から識別情報を認証サーバ（ＡＲ）に伝送し、

d）認証サーバから利用有資格性（正当権限）情報をユーザの通信端末装置に伝送し、上記利用有資格性（正当権限）情報にはユーザの識別性についての情報データが含まれておらず、

e）当該の利用有資格性（正当権限）情報を、ユーザの通信情報端末装置から情報サーバへ伝送し、次いで、該情報サーバは利用有資格性（正当権限）情報の有効性（妥当性）をチェックし、そして、チェック（正誤判定チェック）の肯定的結果（正）がでたときユーザに対して、情報サービスの利用を許可（許容）するようにしたことを特徴とする電子的情報サービス運用者に対するユーザの秘匿性の確保下で電子的情報サービスを利用する方法。

【請求項2】　利用有資格性（正当権限）情報は1つのトランザクションデータ語又はトランザクションデータ語の列から成るようにしたことを特徴とする方法。

【請求項3】　当該のトランザクションデータ語はその都度、利用有資格性（正当使用権限）の検出のため唯一度使用され得、そして当該の一度の利用の後、それの有効性（妥当性）を失うようにしたことを特徴とする方法。

【請求項4】　トランザクションデータ語は、所定の金額に相応するようにしたことを特徴とする方法。

【請求項5】　トランザクションデータ語は1つの所定の利用時間単位に相応するようにしたことを特徴とする方法。

【請求項6】　1つのトランザクションデータ語によっては、所定の提供情報サービスの利用に対して有資格性（正当権限）が与えられるようにしたことを特徴とする方法。

【請求項7】　ユーザ（利用者）の通信端末装置と、情報サーバとの間の接続（路）を次のように仕様設計する、即ち、ユーザの識別性が情報サーバに対して隠れた状態に保持されるように仕様設計することを特徴とする方法。

【請求項8】　利用有資格性(正当権限)情報の有効性（妥当性）が時間的に制限されていることを特徴とする請求項1から7までのうち1項記載の方法。

2

【請求項9】　情報サーバは利用された利用有資格性（正当権限）情報に対する料金決済（清算）情報を認証サーバ（ＡＲ）へ伝送し、ここで、当該の利用有資格性（正当使用権限）情報は、当該の利用の形式についての情報を含んでいないようにしたことを特徴とする方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子的情報サービス運用者に対するユーザの秘匿性の確保下で電子的情報サービスを利用する方法に関する。

【０００２】

【従来の技術】電子的情報サービス、例えば所謂オンライン情報サービス、相互通信型（対話型）ビデオサービス等は急速に重要性を帯びてきている。ここで、その種サービスのユーザはそれのデータの保護権の保持、ことにそのような情報サービスの運用者に対するそれの秘匿性に大きな関心を寄せている。それらのユーザ関心事項の保護は特に、電子的情報サービスの領域にて特別な技術的手法、工夫に基づき、ユーザデータの誤用、乱用の危険が増大しているかである。

【０００３】次に本発明の説明の簡単化のため、通常広帯域ネットワークにおける相互通信型（対話型）相互通信型（対話型）のビデオサービスに就いてのみ言及する。尤も当業者から明らかなように本発明を任意の電気的情報サービス及び任意の、通信端末装置ネットワークと関連して同様に利用し得る。

【０００４】ある1つの加入者向けの相互通信型（対話型）ビデオサービスへのアクセスは、所謂セットトップボックスＳｅｔ－ＴｏｐーＢｏｘ（ＳＴＢ）（要するに、通信端末装置）により行なわれ得、前記セットトップボックスＳｅｔ－ＴｏｐーＢｏｘ は、ネットワーク終端部とテレビ機器との間に設けられている。前記セットトップボックスＳｅｔ－ＴｏｐーＢｏｘ は、広帯域のデータ伝送ネットワーク（一般的には通信ネットワーク）を介してビデオ情報用のメモリ（所謂ビデオサーバ；一般的には情報サーバ）への接続（路）を形成し、そして、その選択及び再生を加入者（ユーザ（利用者））の入力に依存して制御する。

【０００５】ビデオサーバからのビデオー及びマルチメディア情報の呼出はたいていの場合において、コストを要し、而して、そのような機器の民間の運用者（運営者）からの広い提供が可能になる。従って、サービスユーザに対してそれらのコストが考慮され得る手法が可能でなければならない。ここで、データ及び個人性保護の重要性が考慮されねばならない。

【０００６】相互通信型（対話型）ビデオサービス用の現存の試験フィールドにて、及びビデオサービスに対するこれまでの従来可用のソフトウエアにおいて、ビデオサーバにてユーザ（利用者）の識別性がチェックされ、このために、ビデオサーバには次のようなデータが知ら

れていなければならない。名称、アドレス又は銀行接続（路）関係（関連）事項、秘密数（字）ないし番号、識別語。それにより、ビデオネットワークの運用者は基本的に、ユーザ（利用者）の名称をそれの利用関係（関連）事項（例えば呼出された会社、又は会社カテゴリ、利用の頻度）と結合し得る。例えば通信目的のため、そのような情報の乱用に対する防止保護策は、専ら契約上の規制（規定）により行われ得るのであり、技術手段によっては行われ得ない。

【０００７】

【発明が解決しようとする課題】従って、本発明の目的ないし課題とするところは、電子的情報サービス運用者に対するユーザの秘匿性の確保下で電子的情報サービスを利用する有効な方法を提供することである。ここで、相互通信型（対話型）ビデオサービスの利用中心の料金決済（清算）のもとで、電子的情報サービス運用者に対して、ユーザの識別性を秘密にすること（秘匿性）を確保し得るようにするものである。

【０００８】

【課題を解決するための手段】上記課題は、電子的情報サービス運用者に対するユーザの秘匿性の確保下で電子的情報サービスを利用する方法において、特許請求の範囲１の構成要件により解決される。

【０００９】上記方法ではユーザの少なくとも１つの通信端末装置、情報サーバ、認証サーバ間で通信ネットワーク（ＣＮ）を介して接続（路）が形成され、そしてユーザの通信端末装置から識別情報が認証サーバ（ＡＲ）へ伝送される。そこで、認証サーバからは、利用有資格性（正当使用権限）情報がユーザの通信端末装置へ伝送される。上記利用有資格性（正当使用権限）情報はユーザの識別性についての情報を含まない。上記利用有資格性（正当使用権限）情報はユーザの通信端末装置から情報サーバへ伝送される。そこで、上記情報サーバは利用有資格性（正当使用権限）情報をチェックし、そして、正誤判定チェックの肯定的結果（正）のあった際、情報サービスの利用をしてもよいとの許可を与える。

【００１０】本発明によっては、ビデオサービスの運用者（運営者）に対して、ユーザの識別性を秘密にすることが可能になり、然も、利用状況（事情）に応じたコストの料金決済（清算）ないし課金が可能である。この目的のため認証（許可）サーバは顧客の識別性に関して知識を取得（知得）するがビデオサービスにおける利用関係（関連）事項特性についての情報を含まない。

【００１１】本発明の有利な発展形態は従属請求項に規定される。

【００１２】

【実施例】次に図を用いて本発明を有利な実施例に即して説明する。

【００１３】ここで、図中の下記の参照符号を使用する。

【００１４】ＳＴＢ　セットトップボックス（Ｓｅｔ－ＴｏｐーＢｏｘ）、通信端末装置

ＡＲ　　認証（許可）サーバ

ＶＳ　　ビデオサーバ、情報サーバ

ＣＮ　　通信ネットワーク

ＳＵ　　ユーザ、サービスユーザ、加入者

ＵＣ　　ユーザ契約及び相応の料金決済（清算）ないし課金

ＢＣ　　交換媒介契約及び相応の料金決済（清算）ないし課金

ＳＢ　　認証サーバの運用者、交換媒介（業）者（ブローカ、エージェント）

ＳＰ　　サービス提供者、情報サーバの運用者

ｃＡＲ　認証サーバへの接続（路）形成

ａｄ　　認証ダイヤローグ

ｕｉｄ　ユーザの識別

ａｕｔ１　認証、ユーザへの利用有資格性（正当使用権限）情報の伝送

ｃＶＳ　情報サーバへの接続形成

ｓｃｄ　サーバ制御ダイヤローグ

ａｕｔ２　認証の検証、情報サーバへの利用有資格性（正当使用権限）情報の伝送

ａａ　　認証の確認

ｓｃ　　サービスの継続、

ｃＶＡ　情報サーバから認証サーバへの接続（路）形成

ｓａｕｔ　利用有資格性（正当使用権限）情報の伝送

ｃｏｎｆ　ユーザから送信される利用有資格性（正当使用権限）情報の確認のための認証サーバにおける問い合わせ

図１は基礎とされる構成コンフィギュレーションを示す。ユーザはセットトップボックス（Ｓｅｔ－ＴｏｐーＢｏｘ）（一般的には：通信端末装置）はデータネットワーク（一般的には通信ネットワーク）を介して認証（許可）サーバ（ＡＲ）及び、情報サーバの双方と交信する。当該の通信接続部がどのように形成されるかは、本発明にとってどうでもよい。勿論、フレキシブル（融通性のある）接続（路）形成は、例えば、ダイヤリング（選択）接続（路）を介してのものが、好ましい。認証の信頼性を確保するため、情報サーバと認証サーバとの間の情報交換も必要である。以下詳述するように、そのためには情報サーバから認証（許可）サーバへの一方向の情報の流れで事足り、上記情報の流れは本来のビデオサービスの呼出前に、行われ、要するに利用関係（関連）事項についての情報をまだ包含し得ない。

【００１５】図２は、種々のネットワークコンポーネントの提供者間に存在する契約上の関係を示す。ＳＴＢセットトップボックス（Ｓｅｔ－ＴｏｐーＢｏｘ）はその意味で、サービスユーザ（エンドユーザー顧客）により運用（運営）され、情報サーバはサービス提供者（例えばビデオオンデマンド用）により運用（運営）され、そ

して、認証サーバは中立の交換（媒介）一及び料金決済（清算）一企業、例えばネットワーク運用者（運営者）又はクレジットカード経営体により運用される。

【００１６】サービスユーザは認証サーバに知られている。識別化のため認証サーバは秘密数（字）ないし番号を付与する（又は当業者に通有の同等のメカニズムを用いる）。以下秘密数（字）ないし番号（ＰＩＮ＝Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）を介する識別化を基礎とする。但し、本発明は、当該の実施例（態様）に限られるものでない。サービスユーザ（利用者）とサービス提供者との間には直接的な契約上の関係は存しない。サービスに対する料金決済（清算）ないし課金は認証サーバを介してのみ行われる。サービスに対して生じるコストは、認証サーバの運用者（運営者）からサービス提供者へ支払われる。認証サーバとサーバ提供者との間には、同様に、識別化の形態が使用される。当該の識別化の形態は、秘匿性であり、サービスユーザ（利用者）の名称に対する推定を行わせ得ないものである。以下、　当該の秘匿性の識別化のため、任意に選択（選定）されたパスワードが使用されることを基礎とする。

【００１７】図３は、サービスが利用される場合、即ち、例えばフィルムが呼出される場合その時点でのコンポーネント間の通信の経過を示す。ＳＴＢセットトップボックス（Ｓｅｔ－ＴｏｐーＢｏｘ）が情報サーバと接続し得る前に、選択プロセスは、アクセス可能なサーバのうちから行われていなければならず、ここで、サービス交換（媒介、仲介）（時にはブローカと称される）のための特別なコンピュータを用いて当該の選択のプロセスは行われていなければならない。

【００１８】情報サーバをアクセスし得る前に、先ず、認証サーバへの接続が形成されなければならない（ＣＡＲ）。サービスユーザはそれの名称及び交換（媒介、仲介）（業）者と取り極められたＰＩＮにより識別される（ｕｉｄ）。そこで、有効なトランザクションデータ語（例えば実際のテーブルから成る）又は複数のトランザクションデータ語が、セットトップボックス（Ｓｅｔ－ＴｏｐーＢｏｘ）ＳＴＢへ伝送される（ａｕｔ１）。トランザクションデータ語は、例えばテレコム（Ｔｅｌｅｋｏｍ）のドイツＤａｔｅｘ－Ｊ－システム（トランザクションナンバー）では通常であり、例えばホームバンキングの場合通常である。上記トランザクションデータ語はそこで唯一度使用され得る。誤った入力は、少数の試行、試験（テスト）に限られている。本発明に関連して、当業者は、（場合により関連文献を用いて）容易に利用有資格性（正当使用権限）情報の他の形態を使用し得るのであり、このことはそれ自体発明性を有するものでなくてよい。この意味で請求項１においては、利用有資格性（正当使用権限）情報について一般的に規定されている。

【００１９】引き続いて、情報サーバへの接続を形成し得る（ｃＶＳ）、ここで、セットトップボックス（Ｓｅｔ－ＴｏｐーＢｏｘ）ＳＴＢの加入者番号は、隠された状態におかれ得る（ＣＬＩＲ＝Ｃａｌｌｉｎｇ　Ｌｉｎｅ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｒｅｓｔｒｉｃｔｉｏｎ；ＩＳＤＮ及びＢ－ＩＳＤＮにおいて支援される）。本来のサービス（ｓｃ）の展開の前に、ユーザの認証が次のようにして確保される、即ち、セットトップボックス（Ｓｅｔ－ＴｏｐーＢｏｘ）ＳＴＢが情報サーバに（前以て認証サーバから受け取った）トランザクションデータ語を伝送する（ａｕｔ２）。情報サーバは、トランザクションデータ語の有効性（妥当性）をチェックし、それに依存してユーザにサービス利用の許可を与える。

【００２０】勿論、上述の経過は次のことに依存する、即ち情報サーバが許容されたトランザクションデータ語にに対する知識を取得（知得）することに依存する。本発明ではこのことは次のようにして確保される、即ち、トランザクションデータ語が情報サーバにより認証サーバにより任意に設定され、そして、情報サーバと認証サーバとの間の通信を介して調整（整合）されるのである。

【００２１】図４は、相互作用（インタラクション）ないし相互通信型（対話型）情報交換による相互通信可能な手段を示し、当該の上記相互作用（インタラクション）情報交換は、時間的間隔を以て本来のサービス利用に先行し、そして、複数のサービス利用のためにも有効であり得る。ビデオサーバは、認証ベース（例えば、任意に選ばれたトランザクションデータ語の表）を設定し、そして、これを認証サーバに通報する（ｓａｕｔ）。同様に、トランザクションデータ語の生成のため及び接続形成のためのイニシアティブ（主導的機能）は認証サーバから発せられるようにしてもよい。図４に示す手段は特に乱用に対して強い防止機能を有する。それというのは情報サーバは、認証サーバとのコンタクトをはじめる時点で、将来のサービス利用について何等の情報を有し得ないからである。

【００２２】図５には更なる手法を示す。又ビデオサーバが必要な場合にはじめて（サービス利用／フィルム呼出の場合）認証サーバとのコンタクトを行うことも可能である。この場合において、認証サーバはセットトップボックス（Ｓｅｔ－ＴｏｐーＢｏｘ）に供給されるトランザクションデータ語を任意に選び得、そして、ビデオサーバと認証サーバとの間の通信（問い合わせ）は、純然たる問い合わせ（ｃｏｎｆ）である。

【００２３】上述の方法プロセスの種々のさらなる変形が可能であり、その中には以下のものがある。

【００２４】＊サービスに対する利用状況（事情）に応じた料金決済（清算）は種々の手法で確保できる。ユーザの秘匿性（匿名性）は、次のような場合に最も有効に

保護される、即ち付与されたトランザクションデータ語が所定の作業量（サービス）に対する“手形（貸し方）”として解釈されるのである。選択的に、ビデオサーバは認証サーバに、１つのトランザクションデータ語に対する利用済みサービスの総和を（利用時間、フィルムカテゴリ等のような利用詳細事項に関係せずに）通報するとよい。

【００２５】*認証サーバの機能を、相互通信型（対話型）マルチメディアサービスへの規制（規定）アクセスの確実な実施と結びつけて行わせ得る。上記規制アクセスは法律上の枠の条件のもとで要求されるようなものである（例えば米国における“レベル１ゲートウエイ”）。このために、ネットワーク運用（運営者）は、上述の事項プロセスに従って動作するサービス提供者にもに許可を与え得、そして、自ら認証サーバを運用（運営者）しなければならない。このことに対して特に有利であるのは、認証サーバをビデオサーバ（“ブローカ”）に対する選択機能と結合することである。

【００２６】*トランザクションデータ語は、乱用のリスクを更に制限するため、限られた時間に対してだけ“ドロップアウトデータ”の指示によって有効化され得る。

【００２７】本発明は、サービス提供者に対してのサービスユーザの秘匿性の担保のもとで相互通信型（対話型）ビデオサービスの利用を可能にする。これにより、データ保護一規定（データ提供者における利用に関連するデータのみに係わり、個人に係わるデータには係わらない）の維持が可能にされる。更に、本発明はサービス提供者の市場調査において重要な区別的特徴的事項を創出し得る、それというのは、サービスユーザにはデータ乱用によるトラブル、不都合からの、十分な保護防止作用が与えられ得るからである。

【００２８】相互通信型（対話型）ビデオサービスへの規則（規定）アクセス付きネットワークにおいて、本発明はネットワーク運用者（運営者）のコントロールを損なうことなく接続形成（例えば自動選択接続）のための簡単、且つ標準化された方法プロセスを可能にする。

【００２９】

【発明の効果】本発明によれば、電子的情報サービス運用者に対するユーザの秘匿性の確保下で電子的情報サービスを利用する方法を実現（創出）できたという効果が奏され、そして、相互通信型（対話型）ビデオサービスの利用中心の料金決済（清算）のもとで、電子的情報サービス運用者に対して、ユーザの識別性を秘密にすること（秘匿性）を確保することが可能になる当該の方法を実現できたという効果が得られる。

【図面の簡単な説明】

【図１】本発明の有利な実施例の基礎とされるような通信端末装置、認証サーバ及び情報サーバから成る基本構成コンフィギュレーションの概略図である。

【図２】基本構成コンフィギュレーションの通信端末装置とサーバとの間の対応関係及びそれらの間の契約上の関係を示す概念図である。

【図３】本発明の有利な実施例による通信端末装置とサーバとの間の通信の経過の様子を示す概略図である。

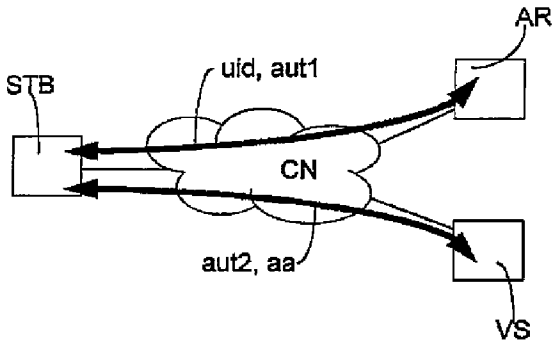
【図４】認証サーバと情報サーバとの間での利用有資格性（正当使用権限）情報の取極めのもとで加入者によるサービス利用前での、認証サーバと情報サーバとの間の通信の経過の様子を示す概略図である。

【図５】サービス利用中での認証問い合わせの際の認証サーバと情報サーバとの間の通信の経過の様子を示す概略図である。

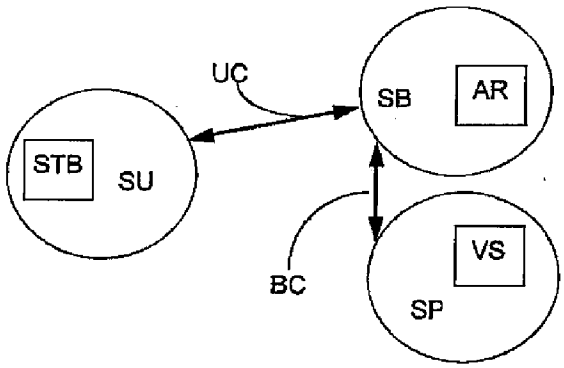
【符号の説明】

ＳＴＢ　セットトップボックス（Ｓｅｔ－Ｔｏｐ－Ｂｏｘ）、通信端末装置
ＡＲ　認証（許可）サーバ
ＶＳ　ビデオサーバ、情報サーバ
ＣＮ　通信ネットワーク
ＳＵ　ユーザ、サービスユーザ、加入者
ＵＣ　ユーザ契約及び相応の料金決済（清算）ないし課金
ＢＣ　交換媒介契約及び相応の料金決済（清算）ないし課金
ＳＢ　認証サーバの運用者、交換媒介(業)者（ブローカ、エージェント）
ＳＰ　サービス提供者、情報サーバの運用者
ｃＡＲ　認証サーバへの接続（路）形成
ａｄ　認証ダイヤローグ
ｕｉｄ　ユーザの識別
ａｕｔ１　認証、ユーザへの利用有資格性（正当使用権限）情報の伝送
ｃＶＳ　情報サーバへの接続形成
ｓｃｄ　サーバ制御ダイヤローグ
ａｕｔ２　認証の検証、情報サーバへの利用有資格性（正当使用権限）情報の伝送
ａａ　認証の確認
ｓｃ　サービスの継続、
ｃＶＡ　情報サーバから認証サーバへの接続（路）形成
ｓａｕｔ　利用有資格性（正当使用権限）情報の伝送
ｃｏｎｆ　ユーザから送信される利用有資格性（正当使用権限）情報の認証のための認証サーバにおける問い合わせ

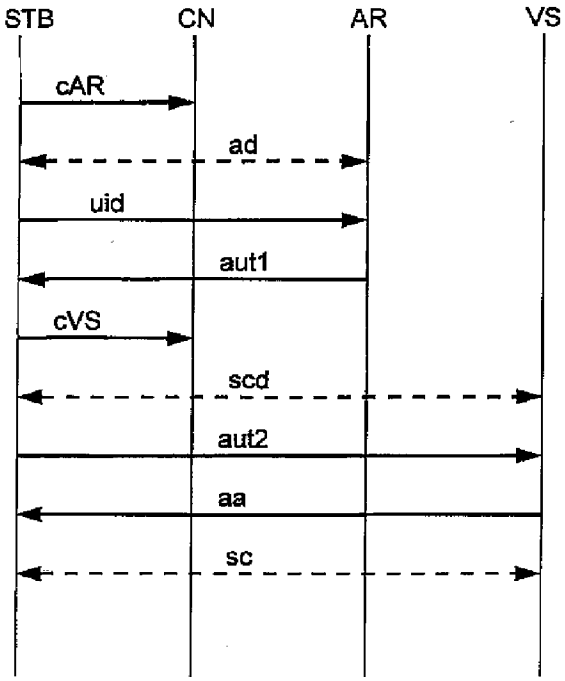
【図1】


AR
STB
uid, aut1
CN
aut2, aa
VS

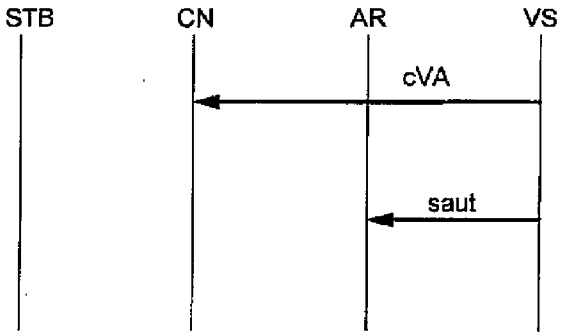
【図2】


UC
SB
AR
STB
SU
BC
VS
SP

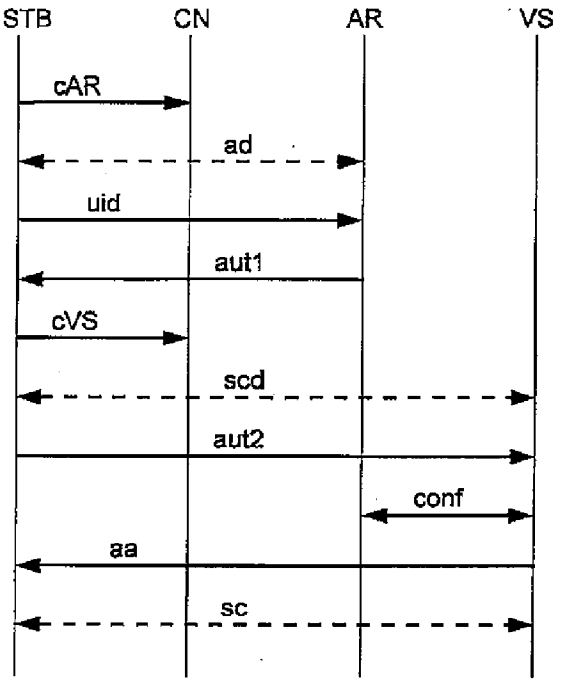
【図3】


STB
CN
AR
VS
cAR
ad
uid
aut1
cVS
scd
aut2
aa
sc

【図4】


STB
CN
AR
VS
cVA
saut

【図5】


STB
CN
AR
VS
cAR
ad
uid
aut1
cVS
scd
aut2
conf
aa
sc